REMARKS

Claims 1-20 are pending in the application.

Claims 6-9 and 12-17 are withdrawn from consideration.

Claims 3, 10-11 and 18-20 are canceled.

Claims 1-2 and 4-5 are currently amended.

Claims 21-24 are new claims.

Independent claim 1 has been amended to more distinctly claim the invention which is an improved method of maintaining privacy of transactions employing a user device having a security module.

The verifying step of the original claim 1 has been replaced with the new verifying step shown below:

> "verifying a proof at the verification computer that the first and second set of signature values are based on the first and second set of values that are obtained from a common value that is unique to the user device;"

Support for this amendment is found on page 9, lines 18-20.

Independent claim 1 has been further amended by adding the limitation shown below which employs a function of the privacy certification authority computer:

> "wherein the privacy certification authority computer uses a base value that is the same for all security modules and for a sufficiently long period such that the privacy certification authority computer can determine a frequency that the security module has requested certification, thereby allowing the privacy certification authority computer to identify whether the security module is a rogue security module."

Support for this amendment is found at page 9, lines 9-12.

Claim 1, as amended, recites an improved method of maintaining privacy for transactions. The improved method maintains the privacy of the user device while, at the same time, it provides the unexpected advantage of identification of rogue security modules. This advantage is not found in any of the methods of maintaining privacy cited in the office action.

The improved method provides this advantage by separating the frequency check used to identify rogue security modules from the request of the service from the verifying party (see page 3, line 15 through page 4, line 5). The two processes are linked through the use of a common value which is unique to the user device (see page 8, lines 25-30.) The verifying party receives a first and second set of signature values, one for verifying trusted access and the other for verifying a frequency check. A privacy certification authority computer performs the frequency check separately from the verifying party so that the verifying party can not learn any identifiable information about the user device other than the fact that both the first and second set of values are linked to the same user device.

In view of this unexpected advantage described above, claim 1, as amended, recites a novel and improved method which overcomes the inability of the prior art methods to identify rogue security modules while maintaining privacy of the transactions of the user device.

35 U.S.C. 112 Rejections

Claims 1-6, 8-12 and 18 were rejected as being indefinite.

Claim 1 had been rejected because the preamble had been interpreted as incorporating the privacy certification authority computers and verification computer into the user device.

Claim 1, as amended, is directed to an improved method of maintaining privacy for transactions employing a user device having a security module. Thus, it does not refer to incorporating the privacy certification authority computers and verification computer into the user device.

Additional amendments were made to clarify the association of a step with a particular device that carries out that step.

Accordingly, rejection of claim 1 for the above reasons is moot.

Several claims had also been rejected for having the phrase "derived from." Applicant has amended claims 1, 2, and 5 by replacing "derived from" with the definite phrase "obtained from." Accordingly claim 1, and claims depending directly or indirectly there from, are definite.

The remaining rejected claims have been either withdrawn or canceled. Accordingly, their rejection is also moot.

35 U.S.C. 102(f) Rejections

Claims 1-5, 10-11, and 18-20 were rejected for incorrect inventive entity. The office action alleges that Anna Lysyanskaya is a co-inventor of the claimed subject matter along with the application's named inventor Jan Camenisch. This conclusion was based on the following references:

(i) "Direct Anonymous Attestation", by Brickell, Camenisch and Chen (herein after D1);

(ii) "A Signature Scheme with Efficient Protocols", by Camenisch and Lysyanskaya (herein after D2); and

(iii) "Signature Schemes and Applications to Cryptographic Protocol Design", by Lysyanskaya (herein after D3).

The applicant respectfully points out that none of D1, D2, and D3 discloses the subject matter sought to be patented in amended claim 1. Amended claim 1 recites an improved method of maintaining privacy for transactions employing a user device having a security module which, unlike the protocols disclosed in D1, D2, and D3, prevents profiling, maintains privacy of transactions performed by the user device, and allows identification of rogue security modules (see page 3, line 15 through page 4, line 5).

D1 discloses the direct anonymous attestation protocol (DAA protocol). D2 and D3 disclose signature schemes similar to the idea underlying the DAA protocol. One of the problems with the DAA protocol disclosed in D1 and the signature schemes disclosed in D2 and D3 is that a verifying party is unable to identify rogue security modules, i.e. security modules which have been compromised and the secret key extracted and published (see page 3, lines 5-12.) In order to identify rogue security modules under the DAA protocol the verifying party must learn use a constant base for some interval of time (see page 3, lines 5-9). However, the drawback to the verifying party using a constant base is that it allows the verifying party to profile the user device and reduces privacy for the user device (see page 3, lines 5-9).

Independent claim 1 as amended recites an improved method of maintaining privacy for transactions which maintains the privacy for the user device while allowing for identification of rogue security modules. The method separates the frequency check used to identify rogue security modules from the request of the service (see page 3, line 15 through page 4, line 5). The two processes are linked through the use of a common value unique to the user device (see page 8, lines 25-30). The verifying party receives two sets of signature values, one for verifying trusted access and the other for verifying a frequency check, but the verifying party does not learn any identifiable information about the user device other than the fact that both sets of values are linked to the same user device. Accordingly, amended claim 1 solves the problem of the DAA protocol's inability to identify rogue security modules while maintaining privacy of the user device.

The references D1, D2 or D3 neither teach nor suggest the instant claims, as amended. Accordingly, Camenisch is the sole inventor of the instant claims, namely claim 1, and claims depending directly or indirectly there from.

35 U.S.C. 103 Rejections

Claims 1-5, 10-11 and 18-20 were rejected in the office action under 35 U.S.C. 103(a) as being unpatentable over "TPM Main Part 1 Design Principles" (herein after D4) in view of "TPM v1.2 Specification Changes" (herein after D5).

First, the applicant respectfully points out that both D4 and D5 disclose only the direct anonymous attestation protocol (DAA protocol). As already discussed under the response to the 102(f) rejection, one of the problems with the DAA protocol is that a verifying party is unable to identify rogue security modules (see D5, page 6, "Trust Considerations"). In order to identify rogue security modules under the DAA protocol, the verifying party must use a constant base for some interval of time. However, this feature does not provide protection against profiling. Therefore, the privacy of the user device is reduced (see D5, page 6, "Named-Base Solution").

Amended claim 1 has the advantage of solving the problem of the DAA protocol's inability to identify rogue security modules while maintaining privacy of the user device.

The DAA protocol's inability to identify rogue security modules while maintaining privacy of the user device is acknowledged in D5 (see D5, page 6, "Trust Considerations"). The solution provided by D5 (see D5, page 6, "Named-Base Solution") permits the verifying party to profile the user device and thus, reduces privacy of the user device. In contrast, the solution provided by the instant claims does not permit the verifying party to profile the user device and thus, maintains privacy of the user device.

Further, there is no suggestion in either D4 or D5 that the Named-Base Solution is still a problem that needs to be solved.

Still further, neither D4 nor D5 provide any teaching or suggestion that would lead to the solution provided by the instant claims and the advantage of maintaining the privacy of the user device while allowing identification of rogue security modules.

Second, the applicant respectfully points out that D4 and D5 do not teach or suggest, either alone or in combination, the following limitations of instant claim 1:

(1) "receiving at the verification computer a second set of signature values generated by the user device using a second set of values obtained from a privacy certification authority computer;"

(2) "checking at the verification computer the validity of the second set of signature values with a public key of the privacy certification authority computer;" and

(3) "verifying a proof at the verification computer that the first and second set of signature values are based on the first and second set of values that are obtained from a common value that is unique to the user device;"

These limitations allow the privacy certification authority computer to perform a separate frequency check and return a separate set of values which can be linked to the first set of values used in attestation by the common value unique to the user device. Therefore, the verifying party does not perform the frequency check and does not learn any information about the user device. All transactions performed by the claimed improved method are not linkable except for transactions with the same privacy certification authority computer for a given period.

Accordingly, D4 and D5 do not teach or suggest, either separately or in combination, each and every limitation of amended claim 1. Furthermore, the absence of these limitations shows that instant claim 1 is not merely a combination of old elements to produce a predictable result (*KSR International Co. v. Teleflex Inc*). Therefore, the office action has failed to establish a *prima facie* case of obviousness.

In view of the preceding, applicants respectfully request that the 35 U.S.C. 112, 35 U.S.C. 102(f), and 35 U.S.C. 103(a) rejections be withdrawn and claim 1, and the claims depending directly and indirectly there from, be allowed.

The Commissioner is hereby authorized to charge any due fees, or credit any overpayments, to Deposit Account No. 090468.

Respectfully submitted,

Date: April 16, 2009

By: /Vazken Alexanian/

Vazken Alexanian
Agent for Applicant(s)
Reg. No. 37,270
IBM Corporation
Intellectual Property Law
T.J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598
Phone: (914) 945-1166